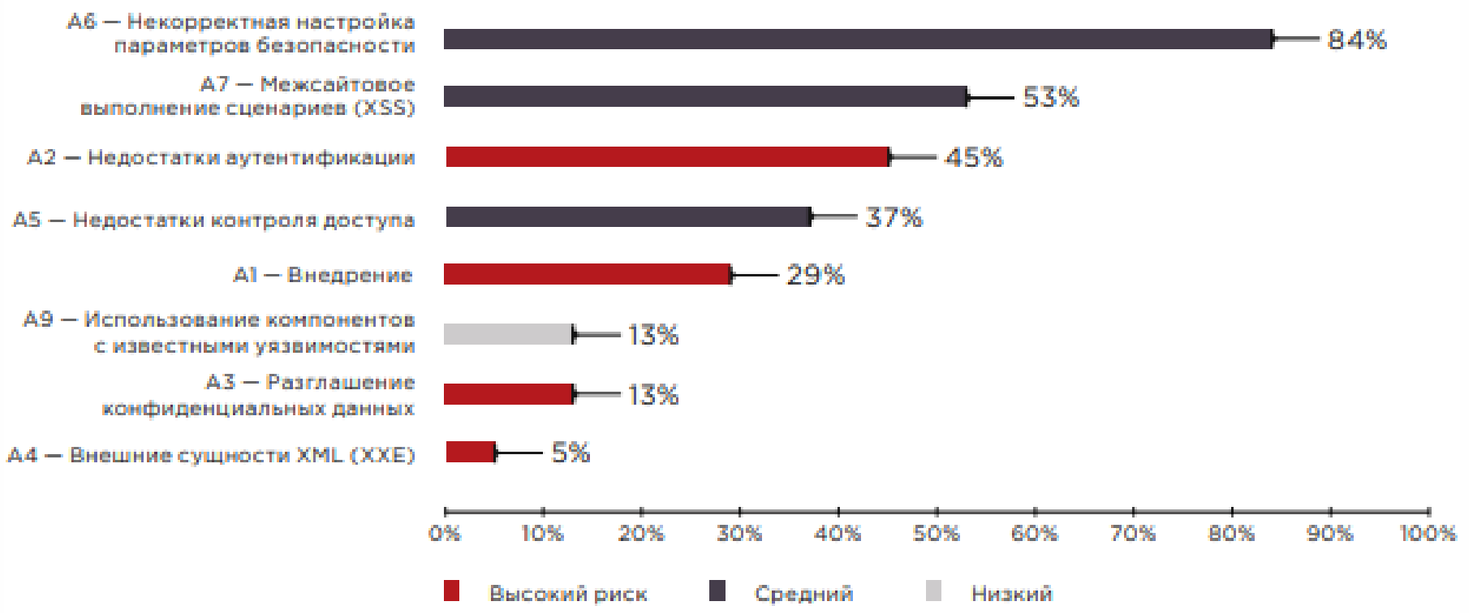
Уязвимости и угрозы веб-приложений



Чаще всех других в 2019 году в веб-приложениях встречались уязвимости, связанные с некорректными параметрами безопасности (Security Misconfiguration). Так, в каждом пятом проанализированном приложении были выявлены уязвимости, позволяющие проводить атаку на сессию, в частности отсутствие флагов HttpOnly и Secure у конфиденциальных Cookie-параметров. С помощью данных недостатков злоумышленник может, например, провести атаку типа «Межсайтовое выполнение сценариев» (Cross-Site Scripting, XSS),чтобы перехватить идентификатор сессии пользователя и от его имени выполнять различные действия в приложении.

В 45% веб-приложений были обнаружены недостатки аутентификации (Broken Authentication). Почти треть выявленных уязвимостей из этой категории — это некорректное ограничение количества неудачных попыток аутентификации. В результате эксплуатации этой уязвимости злоумышленник может подобрать учетные данные пользователя и таким образом получить доступ к веб-приложению. Так, например, для одного приложения потребовалось всего 100 попыток, чтобы успешно войти с правами администратора.

Результаты исследования свидетельствуют о том, что на сегодняшний день не все компании готовы обеспечить надежную защиту персональных данных.

В 16% веб-приложений были найдены критически опасные уязвимости, позволяющие получить контроль не только над приложением, но и над ОС сервера.

**Злоумышленник, получивший контроль над веб-приложением может,
к примеру, внедрить в его код JavaScript-сниффер и продолжить атаку уже на пользователей сайта. Сниффферы могут использоваться для кражи как учетных и персональных данных, так и данных банковских карт. В 2018–2019 годах среди атак на частных лиц наиболее опасными оказались именно атаки с использованием JavaScript-снифферов. Поскольку сниффферы внедряют в код, для того, чтобы их обнаружить, нужно проводить анализ защищенности методом белого ящика.**

В случае целенаправленной атаки на организацию уязвимости веб-приложения могут помочь злоумышленникам получить данные о внутренней сети компании — о структуре сегментов сети, используемых портах, сервисах и т. п. В ряде случаев нарушители даже могут получить доступ к внутренним ресурсам и хранящейся там конфиденциальной информации.

Заключение

Уровень защищенности большинства веб-приложений продолжает оставаться низким. В каждом втором сайте присутствуют уязвимости высокого уровня риска. Впрочем, с каждым годом постепенно снижается доля веб-приложений, содержащих критически опасные уязвимости. Положительная тенденция заключается еще и в том, что компании начинают серьезней относиться к защите веб-приложений, причем не только публичных, но и используемых для внутренних нужд